

CLAIMS

I/We claim:

- [c1] 1. A method in a computing system for conducting an election, comprising:
- for each voter identified by an election worker as being eligible to vote:
 - generating a private key and a public key for the voter;
 - issuing to the voter the only copy of the generated voter private key;
 - signing the generated voter public key with a private key of the election worker who identified the voter;
 - storing a data structure containing the voter public key signed with the election worker private key;
 - enabling the voter to generate a voted ballot by selecting a candidate in at least one election race;
 - encoding the generated voted ballot by executing first distinguished code;
 - decoding the encoded voted ballot by executing second distinguished code;
 - prompting the voter to approve the decoded voted ballot;
 - if the voter approves the decoded voted ballot:
 - encrypting the encoded voted ballot with a single election public key;
 - signing the voted ballot with the voter private key;
 - storing the signed voted ballot for counting;
 - for each stored signed voted ballot:
 - if the signed voted ballot was signed with a private key corresponding to a stored voter public key,

if the stored voter public key was signed with the private key of an election worker whose public key was signed by an election official whose authority derives from an ultimate election authority,

transmitting the unsigned voted ballot to each of a plurality of decryption servers;

receiving from each of the plurality of decryption servers a response containing a partial decryption result;

combining the received responses to obtain a decrypted encoded voted ballot;

decoding the decrypted encoded voted ballot by executing the second distinguished code;

storing the decoded decrypted voted ballot; and

for each stored decoded decrypted voted ballot, tallying the decoded decrypted voted ballots.

[c2] 2. The method of claim 1 wherein the first distinguished code, when executed, accesses a ballot style definition to determine how to encode a voted ballot, and wherein the second distinguished code, when executed, accesses a ballot style definition to determine how to decode a voted ballot.

[c3] 3. A method in a computing system for facilitating the identification of uncounted voted ballots in an election, comprising:

when a voter submits a voted ballot, issuing a value indicating that the voter has submitted a voted ballot;

associating the receipt value with the voted ballot submitted by the voter; and

when the voted ballot submitted by the voter is counted, adding the receipt value to a list of receipt values associated with counted voted ballots,

such that, if the issued receipt value does not appear in the list of receipt values associated with counted voted ballots, the voted ballot with which the missing receipt value is associated may be identified as uncounted.

[c4] 4. The method of claim 3, further comprising storing the issued receipt value in a portable memory device for the voter.

[c5] 5. The method of claim 3, further comprising printing the issued receipt value on a physical object.

[c6] 6. The method of claim 3, further comprising printing the issued receipt value on a physical object in human-readable form.

[c7] 7. The method of claim 3, further comprising printing the issued receipt value on a physical object in machine-readable form.

[c8] 8. The method of claim 3, further comprising printing the issued receipt value on a sheet of paper.

[c9] 9. The method of claim 3, further comprising encoding the issued receipt value in a physical object.

[c10] 10. The method of claim 3, further comprising transmitting the receipt value to a plurality of recipient computer systems, the recipient computer systems each being under the control of a different entity.

[c11] 11. The method of claim 10 wherein the recipient computer systems are selected by the voter.

[c12] 12. The method of claim 3 wherein the receipt number is a public key assigned to the voter.

[c13] 13. The method of claim 3 wherein the receipt number is a public key assigned to the voter, signed with the private key of an election worker who authorized the voter to vote.

[c14] 14. The method of claim 3 wherein the issued receipt value is a signature of the voted ballot using a private key of a vote collection authority.

[c15] 15. The method of claim 14, further comprising publishing a private key corresponding to the private key of a vote collection authority in advance of issuing the receipt value.

[c16] 16. A portable memory device issued to an authorized voter, containing a private key assigned to the authorized voter, such that the portable memory device may be used to authorize a ballot voted by the authorized voter by using the contained private key to sign a representation of the ballot voted by the authorized voter.

[c17] 17. The portable memory device of claim 16 wherein the portable memory device contains the only copy of the private key in existence.

[c18] 18. The portable memory device of claim 16 wherein the portable memory device further contains a public key corresponding to the voter's private key.

[c19] 19. The portable memory device of claim 18 wherein the public key is signed using the private key of a poll worker who authorized the voter.

[c20] 20. The portable memory device of claim 16 wherein the portable memory device further contains receipt information evidencing voting by the voter.

[c21] 21. The portable memory device of claim 16 wherein the contents of the portable memory device comprise a voter certificate.

[c22] 22. A pair of portable memory devices used by a voter, a first portable memory device of the pair containing a private key generated by the voter, a second portable memory device of the pair containing a public key generated by the voter corresponding to the private key contained in the first portable memory device,

such that the first portable memory device may be surrendered to an election official that has approved the voter's participation in the election, enabling the election official to copy the public key into a public key store to evidence the voter's participation in the election without receiving the private key, and such that the second portable memory device may be retained by the voter and used to sign a representation of a ballot cast by the voter.

[c23] 23. A method in a voting station computer system for obtaining a voter's verification of a ballot voted the voter, comprising:

in at least one election race, receiving input from the voter selecting a candidate in the race;

in response to the input from the voter, generating a first internal representation of the voted ballot;

translating the first internal representation of the voted ballot into an external representation of the voted ballot;

translating the external representation of the voted ballot into a second internal representation of the voted ballot;

using the second internal representation of the voted ballot to generate a confirmation display showing the candidates selected by the voter; and

if and only if the voter grants confirmation of the confirmation display, transmitting the external representation of the voted ballot to another computer system for storage.

[c24] 24. The method of claim 23 wherein translating the external representation of the voted ballot into a second internal representation of the voted ballot is performed by executing a distinguished body of code, the method further comprising, in a computer system other than the voting station computer system, executing the distinguished body of code to translate the external representation of the voted ballot into a third internal representation of the voted ballot.

[c25] 25. The method of claim 24, further comprising tallying the third internal representation of the voted ballot.

[c26] 26. The method of claim 24, further comprising verifying that the distinguished body of code executed in the voting station computer system is the same as the distinguished body of code executed in the computer system other than the voting station computer system.

[c27] 27. The method of claim 24 wherein the distinguished body of code is executed on the computer system to which the external representation of the ballot for the voter is transmitted.

[c28] 28. The method of claim 24 wherein the distinguished body of code is executed on a computer system other than the voting station computer system, and other than the computer system to which the external representation of the voted ballot is transmitted.

[c29] 29. A computer-readable medium whose contents cause an originating computer system to verify user input by:

- receiving user input;
- generating a first internal representation of the user input;
- translating the internal representation of the user input into an external representation of the user input;
- translating the external representation of the user input into a second internal representation of the user input;
- using the second internal representation of the user input to generate a confirmation display showing the user input; and
- if and only if the user grants confirmation of the confirmation display, transmitting the external representation of the user input to a destination computer system for processing.

[c30] 30. The method of claim 29 wherein translating the external representation of the user input into a second internal representation of the user input is performed by executing a distinguished body of code in the originating computer system, and wherein the contents of the computer-readable medium further cause a destination computer system to:

- execute the distinguished body of code to translate the external representation of the user input into a third internal representation of user input;
- and
- process the third internal representation of the user input.

[c31] 31. A method in a computing system for completing a blank ballot, comprising:

- displaying a list of two or more candidates;
- receiving first user input selecting a first one of the candidates;
- in response to receiving the first user input, displaying an indication that the first candidate is selected;

after receiving the first user input, receiving second user input selecting a second one of the candidates;

in response to receiving the second user input, continuing to display an indication that the first candidate is selected;

after receiving the second user input, receiving third user input deselecting the first candidate;

in response to receiving the third user input, displaying an indication that no candidate is selected;

after receiving the third user input, receiving fourth user input selecting the second candidate; and

in response to receiving the fourth user input, displaying an indication that the second candidate is selected.

[c32] 32. The method of claim 31, further comprising issuing a voted ballot on which the second candidate is selected.

[c33] 33. The method of claim 31, further comprising, in response to receiving the second user input, displaying an indication that the currently-selected candidate must be deselected before another candidate may be selected.

[c34] 34. The method of claim 31 wherein the first, second, third, and fourth user input is received from a user via a touch display.

[c35] 35. A method in a computing system for completing a blank ballot, comprising:

displaying a list of candidates, none of which is initially selected, up to a maximum number of which may be selected;

receiving instances of user input each identifying a candidate on the list;

in response to receiving an instance of user input identifying a candidate from the list:

if the identified candidate is presently selected, updating the displayed list of candidates to deselect the identified candidate;

if the identified candidate is not presently selected, if the maximum number of candidates are not presently selected, updating the displayed list of candidates to select the identified candidate; and

if the identified candidate is not presently selected, if the maximum number of candidates are presently selected, maintaining the displayed list of candidates unchanged.

[c36] 36. The method of claim 35, further comprising, in response to receiving an instance of user input identifying a candidate from the list, if the identified candidate is not presently selected, if the maximum number of candidates are presently selected, displaying an indication that a candidate must be deselected before any additional candidates may be selected.

[c37] 37. The method of claim 35 wherein the maximum number is one.

[c38] 38. The method of claim 35 wherein the maximum number is greater than one.

[c39] 39. A method in a computing system for completing a blank ballot, comprising:

displaying a list of two or more candidates;

receiving first user input selecting a first one of the candidates;

in response to receiving the first user input, displaying an indication that the first candidate is selected;

after receiving the first user input, receiving second user input selecting a second one of the candidates; and

in response to receiving the second user input, displaying a warning indicating that the selection of the first candidate is being changed to the selection of a second candidate.

[c40] 40. A method in a computing system for casting a ballot, comprising:
receiving user input selecting one candidate in each of a plurality of races;
simultaneously displaying (a) an indication of each candidate selected by the user input, and (b) a control for approving the selections; and
casting the ballot only in response to operation of the control for approving the selections.

[c41] 41. The method of claim 40, further comprising:
displaying a control for modifying the selections; and
if the control for modifying the selections is operated, enabling the user to provide additional user input modifying the selection of the candidates.

[c42] 42. A method for facilitating voting by a voter, comprising:
at a registration station:
verifying the voter's identity;
if the voter's identity as verified qualifies the voter to vote, providing to the voter a portable memory device connoting the voter's individuated right to vote;
at a voting station:
accessing the portable memory device to discern the voter's individuated right to vote;
enabling the voter to select one of a plurality of candidates in each of one or more election races; and
producing for the voter a physical receipt evidencing the voter's voting.

[c43] 43. A method in a computing system for storing in a storage device records containing information derived from voted election ballots, comprising:

receiving a plurality of records, each record containing information derived from one of a plurality of voted election ballots; and

for each received record:

selecting a random location in the storage device at which to store the record using a hardware random-number generator; and

storing the record at the selected random location, thus dissociating the positions of the records in the storage device from the order in which the records are received.

[c44] 44. The method of claim 43 wherein the records are stored on a magnetic medium.

[c45] 45. The method of claim 43 wherein the records are stored on a hard drive.

[c46] 46. The method of claim 43 wherein the records are stored on a removable medium.

[c47] 47. The method of claim 43 wherein the records are stored in programmable read-only memory.

[c48] 48. The method of claim 43 wherein the records are stored in random access memory.

[c49] 49. The method of claim 43 wherein the records are stored in a database.

[c50] 50. The method of claim 43, further comprising splitting each received record into a first portion and a second portion, and wherein the first portion of each record is stored in a database, and wherein the first portion of each record is stored in a file system file.

[c51] 51. The method of claim 43, further comprising selecting the randomly-selected location using a random-number generator.

[c52] 52. A computer memory containing a sequential series of entries, each entry capable of containing a record of the voting of a single voter among a plurality of voters, a record of the voting of each voter of the plurality being stored in a randomly-selected entry in the series of entries, such that records of the voting of particular voters may not be identified based upon the locations of the entries containing the records of the voting.

[c53] 53. A method in a computing system for tracking a voted ballot during processing, comprising:

receiving the voted ballot, the received voted ballot being encoded, then encrypted, then signed with a private key generated for the voter voting the voted ballot;

separating the signature from the encoded and encrypted voted ballot;

identifying the signature and the encoded and encrypted voted ballot without signature in such a way that an association is maintained between the signature and the encoded and encrypted voted ballot without signature;

decrypting the encoded and encrypted voted ballot without signature;

identifying the encoded and decrypted voted ballot in such a way that an association is maintained between the signature and the encoded and decrypted voted ballot;

decoding the encoded and decrypted voted ballot;

identifying the decoded voted ballot in such a way that an association is maintained between the signature and the decoded voted ballot,

such that the signature of the received voted ballot may be accessed based on the identification of the decoded voted ballot to correlate the decoded voted ballot with the voter voting the voted ballot, using a public key generated for the voter voting the voted ballot.

[c54] 54. A computer-readable medium whose contents cause a computing system to track a voted ballot during processing, comprising:

receiving the voted ballot, the received voted ballot being encoded, then signed with a private key generated for the voter voting the voted ballot;

separating the signature from the encoded voted ballot;

identifying the signature and the encoded voted ballot without signature in such a way that an association is maintained between the signature and the encoded voted ballot without signature;

decoding the encoded voted ballot without signature;

identifying the decoded voted ballot in such a way that an association is maintained between the signature and the decoded voted ballot,

such that the signature of the received voted ballot may be accessed based on the identification of the decoded voted ballot to identify the sanctioned election worker signing the voted ballot to correlate the decoded voted ballot with the voter voting the voted ballot, using a public key generated for the voter voting the voted ballot.

[c55] 55. A method in a computing system for determining election results, comprising:

receiving a plurality of cast ballots, each cast ballot having a certification provided by a particular election official connoting the approval of the voter casting the ballot; and

for each received cast ballot, counting the cast ballot only if the certification of the cast ballot can be uninterruptedly traced back to an election official who is the ultimate certification authority for voter approval.

[c56] 56. The method of claim 55 wherein each received cast ballot designates, for each of a plurality of election races, up to one voted-for candidate, and wherein counting a cast ballot includes incrementing a total of votes cast for each candidate designated by the cast ballot as voted-for.

[c57] 57. The method of claim 55 wherein each election official providing a certification of a cast ballot has a private encryption key, the method further comprising certifying each cast ballot by signing a public key of the voter casting the cast ballot with a private key of the election official providing a certification of the cast ballot.

[c58] 58. The method of claim 55 wherein electronic cast ballots are received.

[c59] 59. A method in a computing system for determining election results, comprising:

receiving a plurality of cast ballots, each cast ballot having a certification connoting the approval of the cast ballot by the voter casting the ballot; and

for each received cast ballot, counting the cast ballot only if the certification of the cast ballot is among a set of certifications issued to voters by an election authority.

[c60] 60. The method of 59, further comprising determining whether the certification of the ballot is among a set of certifications issued to voters by an election authority by determining if the cast ballot is signed by a private key corresponding any of a set of public keys each corresponding to a private key issued to a voter to connote the voter's eligibility to vote.

[c61] 61. The method of 59, further comprising determining whether the certification of the cast ballot is among a set of certifications issued to voters by an election authority by:

determining if the cast ballot is signed by a private key corresponding any of a set of public keys each corresponding to a private key issued to a voter to connote the voter's eligibility to vote; and

determining whether a public key corresponding the private key with which the cast ballot is signed has been signed with the private key of an authorized election official.

[c62] 62. The method of claim 59 wherein each received cast ballot designates, for each of a plurality of election races, up to one voted-for candidate, and wherein counting a ballot includes incrementing a total of votes cast for each candidate designated by the ballot as voted-for.

[c63] 63. A method of determining whether a ballot style is proper to use in an election, comprising:

accessing a ballot style authorization policy established for the election, the authorization policy referencing an authority structure established for the election;

accessing a record of an authorization process performed for the ballot style, the record of the authorization process referencing the authority structure; and

determining that the ballot style is proper to use in the election only if the record of an authorization process indicates that the authorization process was performed in accordance with the authorization policy.

[c64] 64. The method of claim 63 wherein the authority structure established for the election is a public key infrastructure.

[c65] 65. The method of claim 63 wherein the accessed record of an authorization process performed for the ballot style is attached to the ballot style.

[c66] 66. The method of claim 63 wherein the accessed record of an authorization process performed for the ballot style is one or more cryptographic signatures of the ballot style.

[c67] 67. A method for conducting an election, comprising:
establishing a public key infrastructure for use in an election; and
employing the established public key infrastructure in the operation of a voting site.

[c68] 68. The method of claim 67 wherein the established public key infrastructure is employed in the operation of a physical voting site.

[c69] 69. The method of claim 67 wherein the established public key infrastructure is employed in the operation of a virtual voting site.

[c70] 70. The method of claim 67 wherein the public key infrastructure includes an authority tree for authorizing voters to vote in the election.

[c71] 71. The method of claim 70 wherein the root of the authority tree is an entity with ultimate responsibility for voter authorization.

[c72] 72. The method of claim 70 wherein the root of the authority tree is an individual with ultimate responsibility for voter authorization.

[c73] 73. The method of claim 70 wherein the root of the authority tree is a group with ultimate responsibility for voter authorization.

[c74] 74. The method of claim 70 wherein the leafs of the authority tree are authorized voters.

[c75] 75. The method of claim 70 wherein the parents of leafs in the authority tree are election workers who directly authorize voters.

[c76] 76. The method of claim 70 wherein the non-root ancestors of the parents of leafs in the authority tree are intermediary election officials.

[c77] 77. The method of claim 70, further comprising, for each non-root node of the authority tree, storing a public key of the node, signed by a private key of the parent of the node, such that, for an authorized voter, there is stored a public key of the authorized voter signed by an election worker, a public key of the election worker's signed by a descendent of an ultimate authority for voter authorization, and, for nodes in a path between the ultimate authority and the descendent of the ultimate authority, a public key of the child node signed with a private key of the parent node.

[c78] 78. The method of claim 67 wherein the public key infrastructure includes an authority tree for approving a ballot style for the election.

[c79] 79. The method of claim 78, further comprising using the authority tree to approve a ballot style for the election in accordance with an approval policy established for the election.

[c80] 80. The method of claim 79, further comprising storing details of the approval process.

[c81] 81. The method of claim 80, further comprising auditing the authorization of a ballot style by using the stored details to determine whether the

authority tree was used to approve a ballot style for the election in accordance with the approval policy.

[c82] 82. The method of claim 79 wherein the approval policy requires that the ballot style be signed by at least a minimum number of nodes in the authority tree having a particular quality.

[c83] 83. A method in a computing system for casting a ballot, comprising:
storing data including a reference to a public key generated for a voter; and
signing data representing a ballot voted by the voter with a private key generated for the voter.

[c84] 84. The method of claim 83 wherein the data including a reference to the public key generated for the voter that is stored is signed with a private key of a poll worker identifying the voter as eligible to vote, thus demonstrating that the voter is an eligible voter.

[c85] 85. The method of claim 83 wherein the reference to the public key generated for the voter included in the stored data is a copy of the public key generated for the voter.

[c86] 86. The method of claim 83 wherein the reference to the public key generated for the voter included in the stored data is a pointer to the public key generated for the voter.

[c87] 87. The method of claim 83 wherein the reference to the public key generated for the voter included in the stored data is an identifier associated with the public key generated for the voter.

[c88] 88. The method of claim 83 wherein the reference to the public key generated for the voter included in the stored data is an index to the public key generated for the voter.

[c89] 89. The method of claim 83, further comprising applying the public key generated for the voter to the signed ballot to demonstrate that the private key was used to sign the data representing the voted ballot, and thus that the voted ballot represented by the signed data was cast by the voter.

[c90] 90. The method of claim 83, further comprising applying the public key generated for the voter to the signed voted ballot to demonstrate at a time after the data representing the voted ballot is signed that the data representing the voted ballot is identical to the data representing the voted ballot at the time it was signed, and was not modified in the interim.

[c91] 91. The method of claim 83, further comprising generating the public key and the private key for the voter.

[c92] 92. The method of claim 91 wherein the public key and the private key are generated in response to a command issued by a poll worker identifying the voter as eligible to vote, but the private key is inaccessible to the poll worker.

[c93] 93. The method of claim 83 wherein the public key and the private key are generated by the voter, further comprising receiving the public key from the voter.